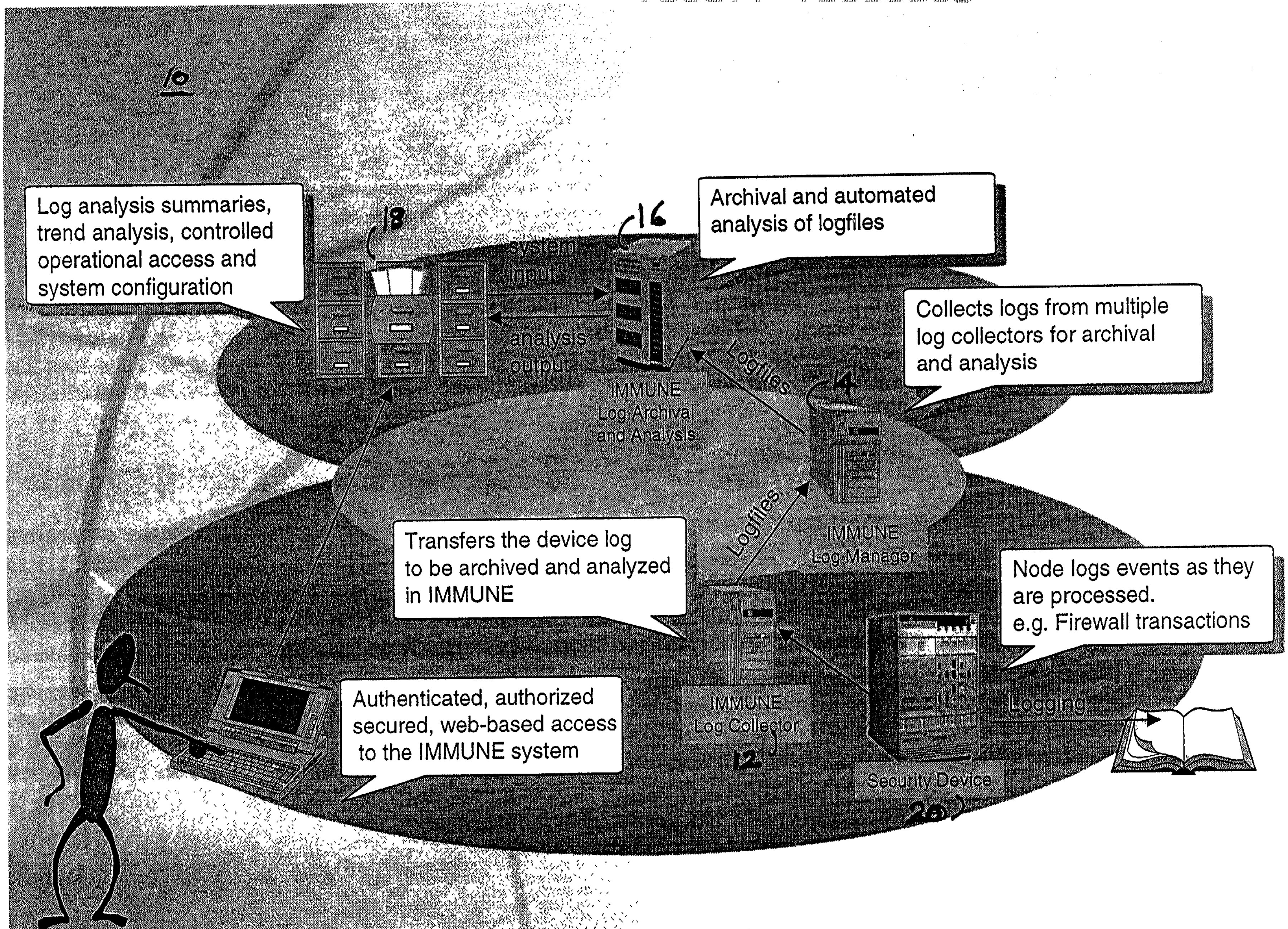
10
Log analysis summaries, trend analysis, controlled operational access and system configuration
18
system input
analysis output
16
Archival and automated analysis of logfiles
IMMUNE Log Archival and Analysis
Logfiles
14
Collects logs from multiple log collectors for archival and analysis
Logfiles
IMMUNE Log Manager
Transfers the device log to be archived and analyzed in IMMUNE
Node logs events as they are processed. e.g. Firewall transactions
Authenticated, authorized secured, web-based access to the IMMUNE system
IMMUNE Log Collector
12
Logging
Security Device
20

FIGURE 1

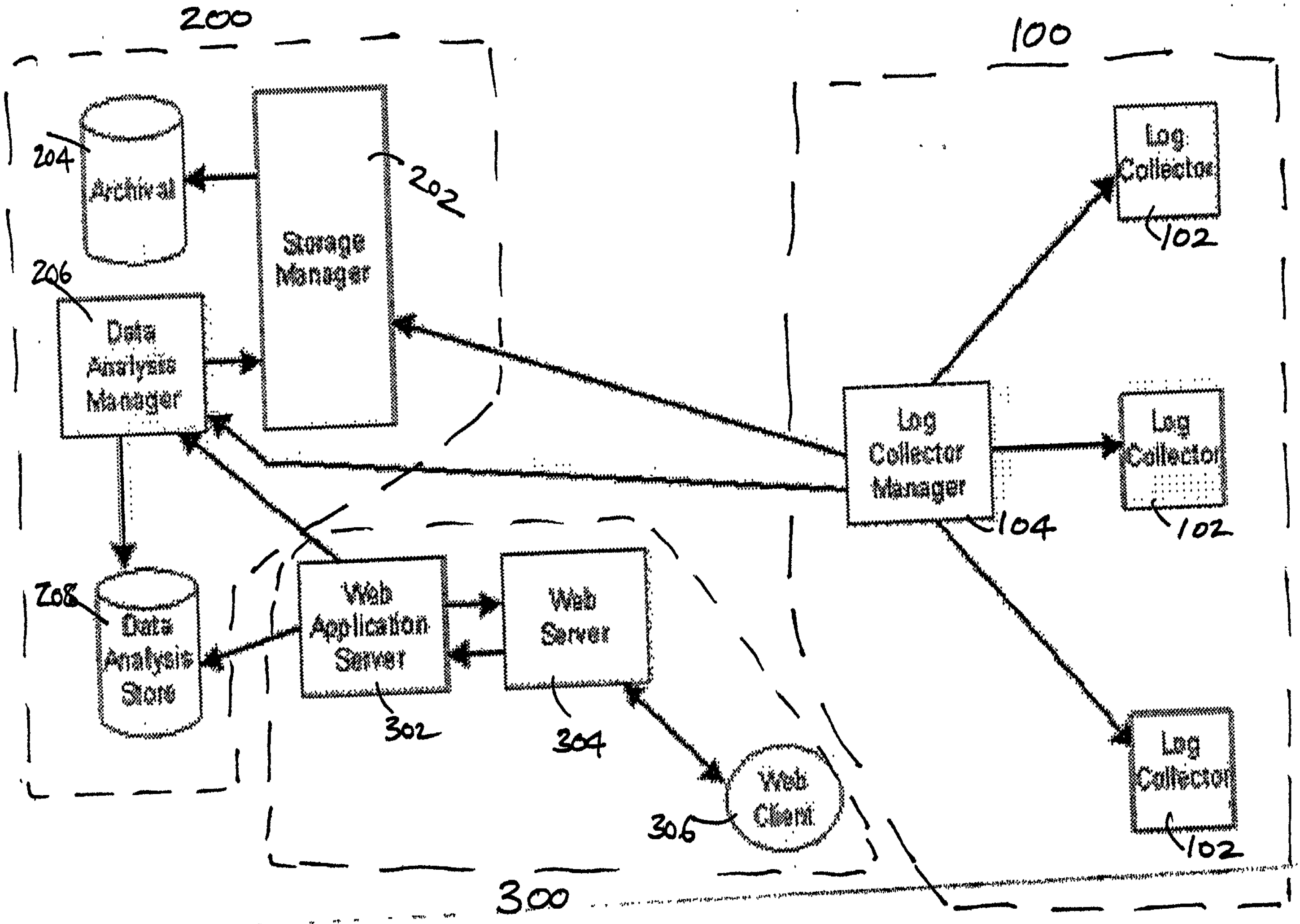

200
100
204
Archival
Storage Manager
202
206
Data Analysis Manager
Log Collector
102
Log Collector Manager
Log Collector
102
104
208
Data Analysis Store
Web Application Server
Web Server
302
304
Log Collector
Web Client
306
102
300

FIGURE 2.

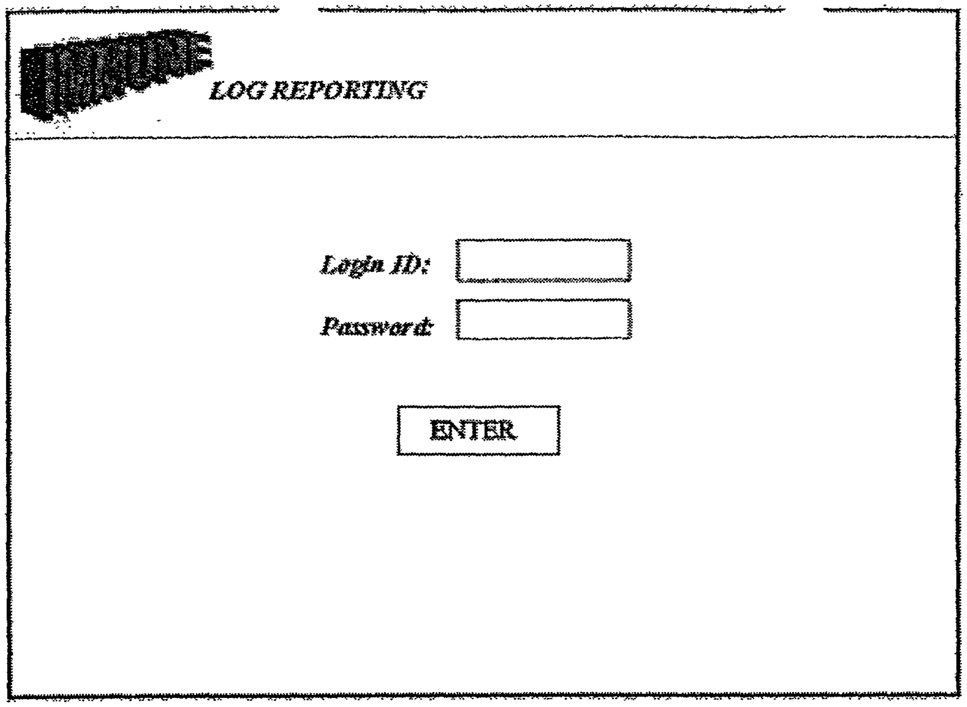


FIGURE 3

This is the Main Menu

Although all the tabs appear on this example, each individual will only get a subset of these tabs based on the status assigned to their userid

Initially none of the tabs are selected

Once a tab has been selected, the menu gets replaced with the menu of tabs that have been set up for that particular

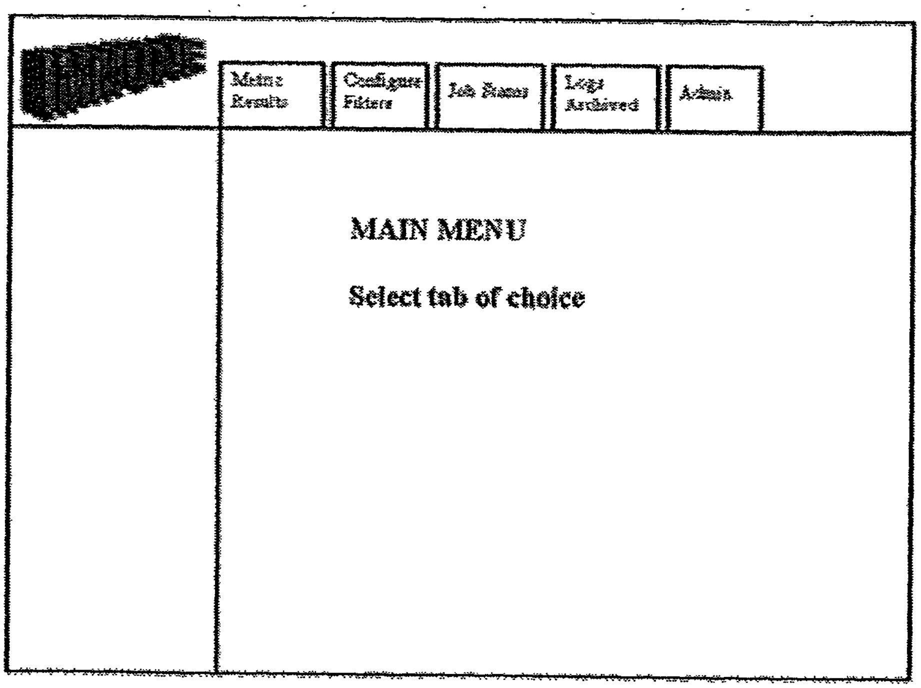


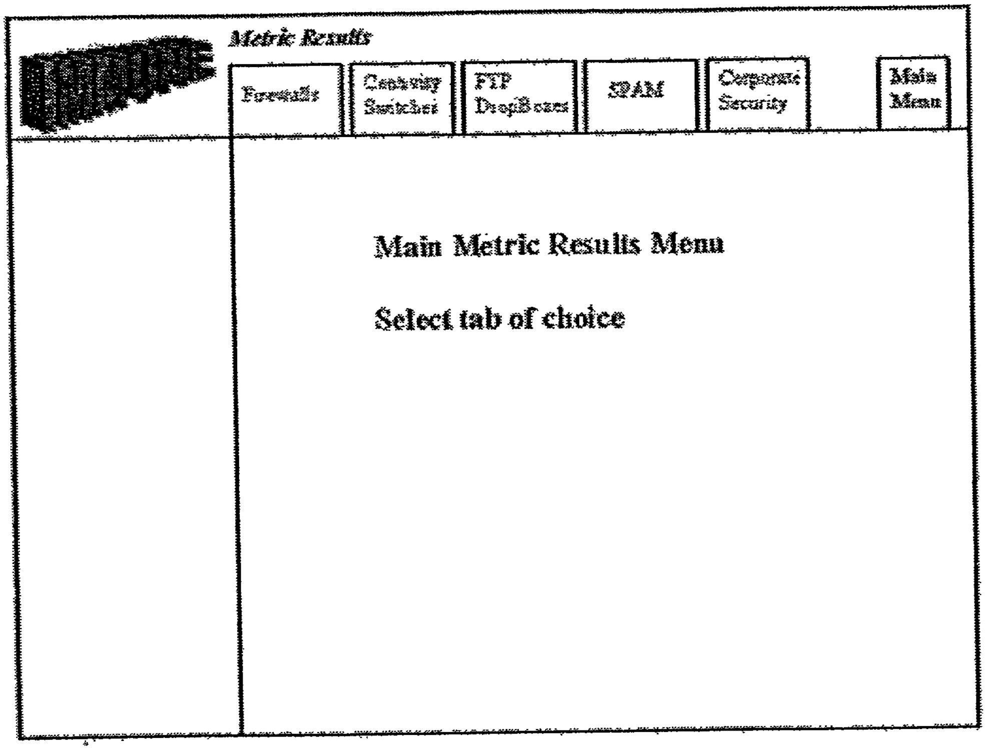
FIGURE 4

This is the Main Results Menu

Although all the tabs appear in this example, each individual will only get a subset of these tabs based on the status assigned to their userid

Initially none of the tabs are selected

Once a tab has been selected the menu gets replaced with the menu of tabs that have been set up for that particular



Metric Results

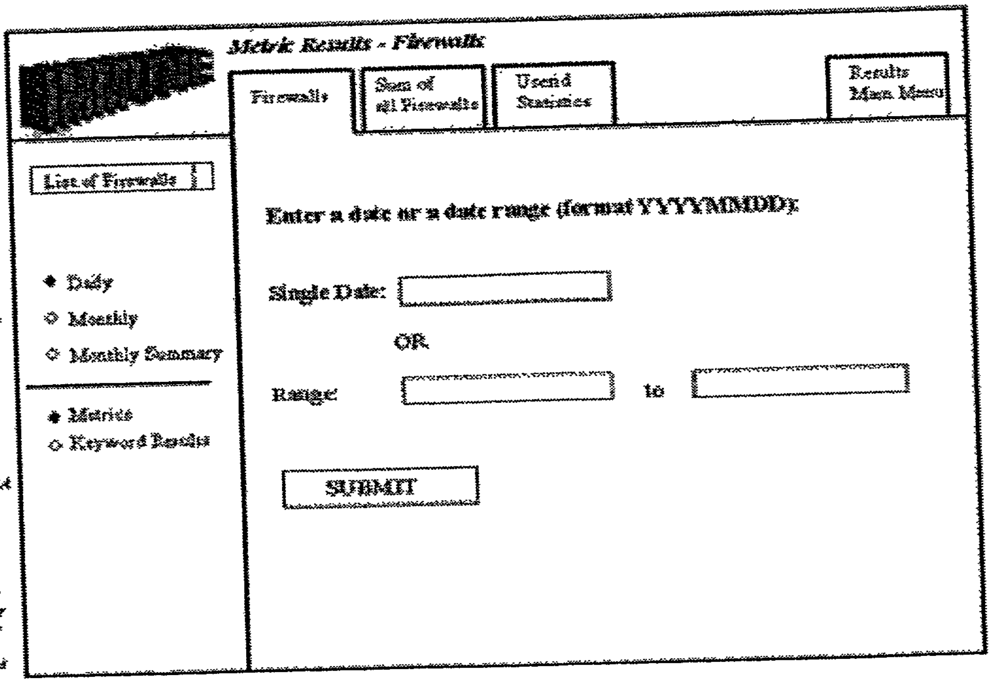
Firewalls | Centricity Switches | FTP DropBoxes | SPAM | Corporate Security | Main Menu

Main Metric Results Menu

Select tab of choice

FIGURE 5.

This is the first window that will appear when firewalls are selected from the main menu. The user would also choose this tab if they want to look at another date or firewall The user can enter the date and firewall information that they want to look at. They could also choose to review the other firewall elements available by clicking on the different tabs across the top. Please note that the SHADOWO tab will only appear if the userid doing the viewing has permission to do DBA type things.. Any time the user changes the daily, monthly, monthly summary radio buttons, they will be prompted to re-enter a date. If a monthly button is selected, they the dates would only by year and month



Metric Results - Firewalls

Firewalls | Sum of all Firewalls | Userid Statistics | Results Main Menu

List of Firewalls

● Daily
○ Monthly
○ Monthly Summary

● Metrics
○ Keyword Results

Enter a date or a date range (format YYYYMMDD):

Single Date: [ ]

OR

Range: [ ] to [ ]

SUBMIT

FIGURE 6

The date that was selected by the previous window appears on the left as the date or range of dates field.

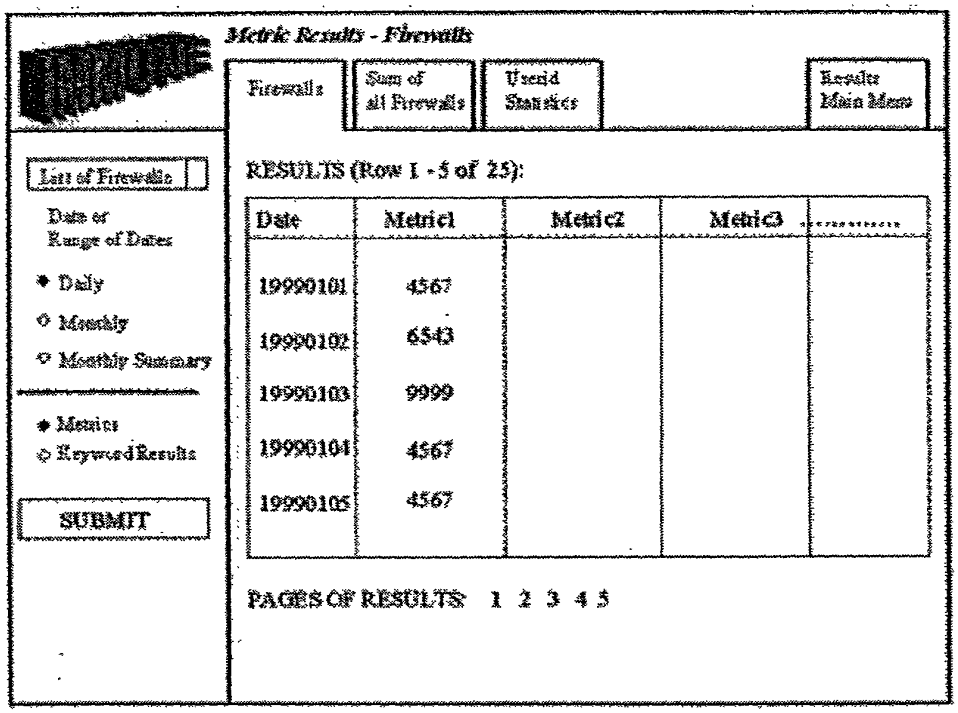
The results on the right only appears once the submit button has been pressed

Any change to the info on the left will clear the results displayed until another SUBMIT has been done.

The last page would have a total if helpful.

If there are more metrics than will appear on the screen, there will be a scrollbar

This example shows what will be displayed for metrics.



Metric Results - Firewalls

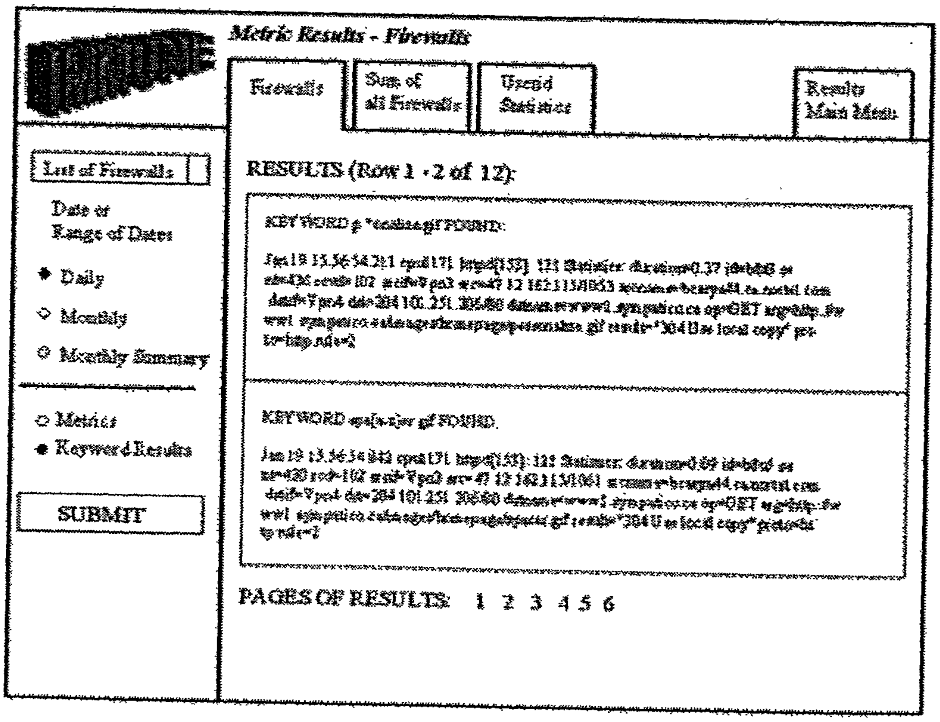
RESULTS (Row 1 - 5 of 25):

Date	Metric1	Metric2	Metric3	....
19990101	4567			
19990102	6543			
19990103	9999			
19990104	4567			
19990105	4567			

PAGES OF RESULTS: 1 2 3 4 5

FIGURE 7.

This page shows what will be displayed if the user wants to look at keyword results



Metric Results - Firewalls

RESULTS (Row 1 - 2 of 12):

```
KEYWORD g *[illegible].gif FOUND:

Jan 19 13:56:34:211 cpsd171 httpd[155]: 121 Statistics: duration=0.37 id=[illegible] st
=[illegible] code=102 [illegible] pa3 [illegible] 12 162.113.[illegible] [illegible].ca.[illegible].com
[illegible] pa4 [illegible]=204.101.251.306:80 [illegible]=www1.sympatico.ca op=GET [illegible]:/fw
ww1.sympatico.ca/[illegible].gif [illegible]="304 Use local copy" pr-
[illegible]=http rd=2

KEYWORD [illegible].gif FOUND.

Jan 19 13:56:34:843 cpsd171 httpd[155]: 121 Statistics: duration=0.69 id=[illegible] st
=420 rc=102 [illegible]pa3 [illegible] 12 162.113.[illegible] [illegible].ca.[illegible].com
[illegible] pa4 [illegible]=204.101.251.306:80 [illegible]=www1.sympatico.ca op=GET [illegible]:/fw
ww1.sympatico.ca/[illegible].gif [illegible]="304 Use local copy" protocol=
[illegible] rd=2
```

PAGES OF RESULTS: 1 2 3 4 5 6

FIGURE 8

The month that was selected by the previous window appears on the left in the month or range of months field

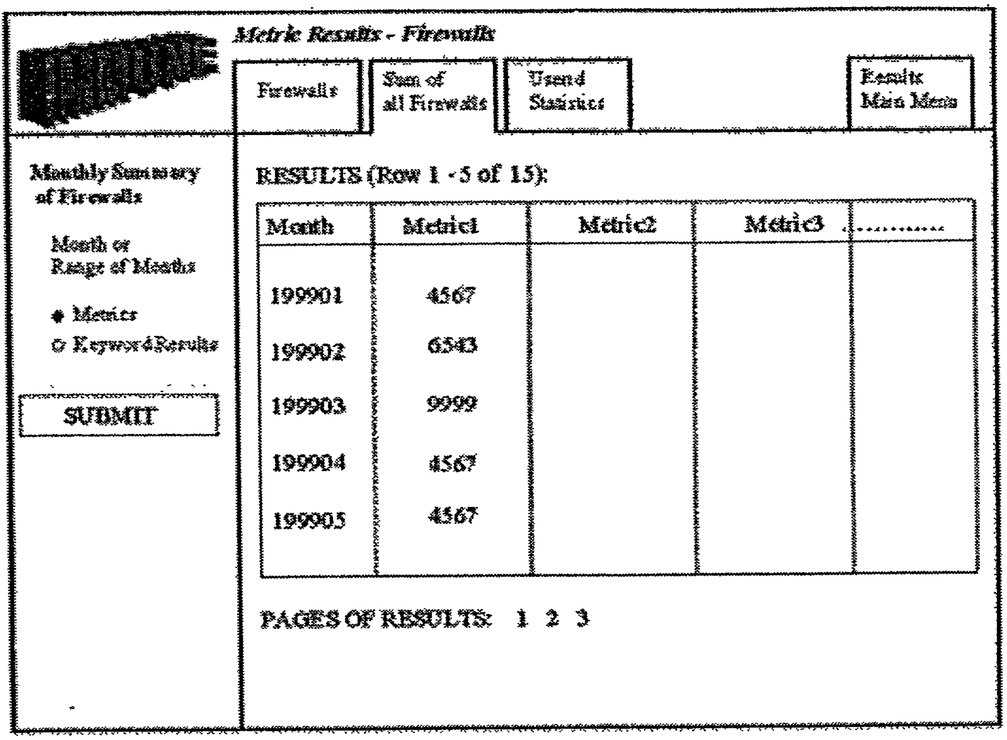
The results on the right only appears once the submit button has been pressed

Any change to the info on the left will clear the results side until another SUBMIT has been done

The last page could have a total if helpful

If there are more metrics than will appear on the screen, there will be a scrollbar.

This example shows what will be displayed for metrics



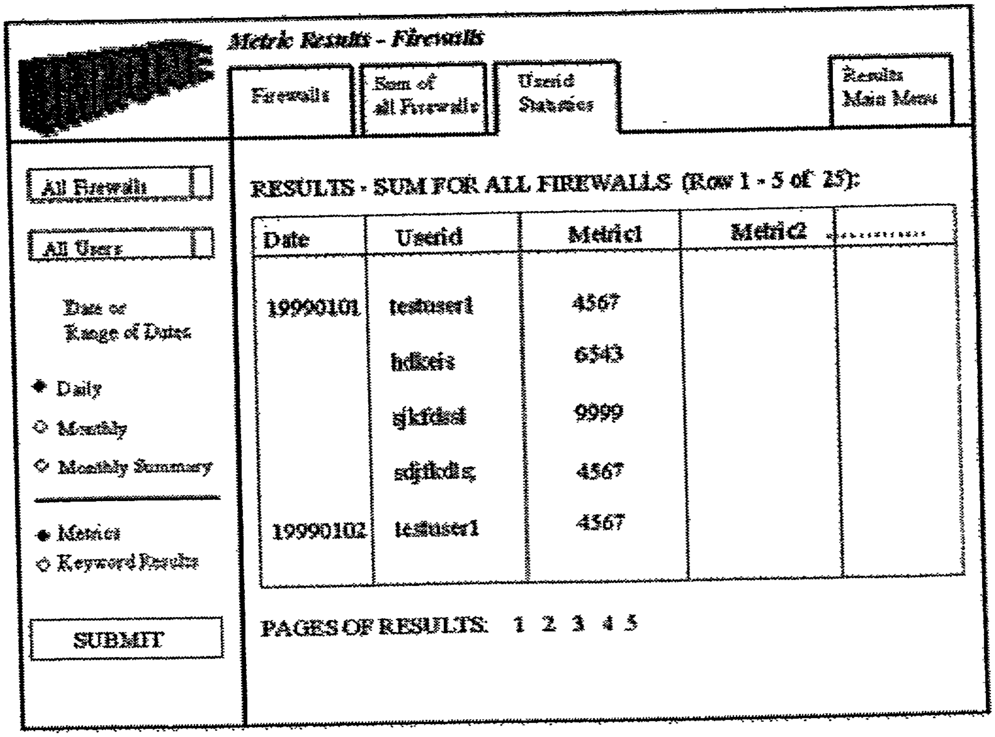
RESULTS (Row 1 - 5 of 15):

Month	Metric1	Metric2	Metric3	....
199901	4567			
199902	6543			
199903	9999			
199904	4567			
199905	4567			

PAGES OF RESULTS: 1 2 3

FIGURE 9

Once the user has selected a date, they must then select a firewall and user
The example on the right shows how the information will be displayed if the user chooses all firewalls and all users
The results will show a line for each user for each date.
The metrics displayed will be a sum for all firewalls.



RESULTS - SUM FOR ALL FIREWALLS (Row 1 - 5 of 25):

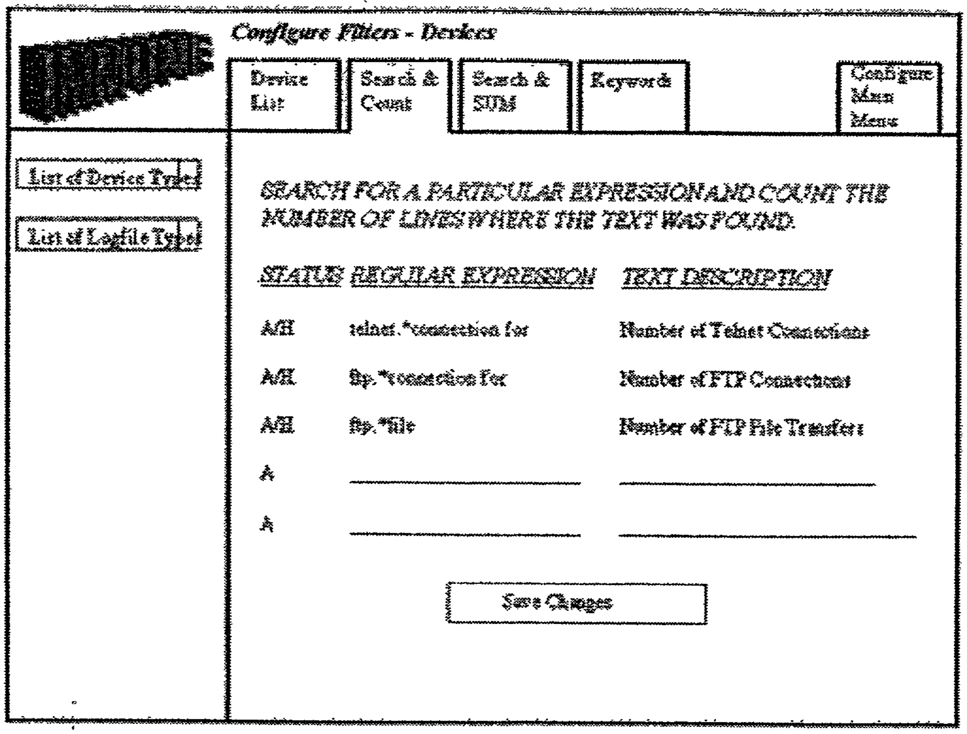
Date	Userid	Metric1	Metric2	....
19990101	testuser1	4567		
	hdkeis	6543		
	sjkfdsd	9999		
	sdjtkdis	4567		
19990102	testuser1	4567		

PAGES OF RESULTS: 1 2 3 4 5

FIGURE 10

Once a regular expression has been added, it cannot be changed however the text description and status can.

When adding a new expression the status is set to ACTIVE



Configure Filters - Devices

Device List | Search & Count | Search & SUM | Keywords | Configure Main Menu

List of Device Types

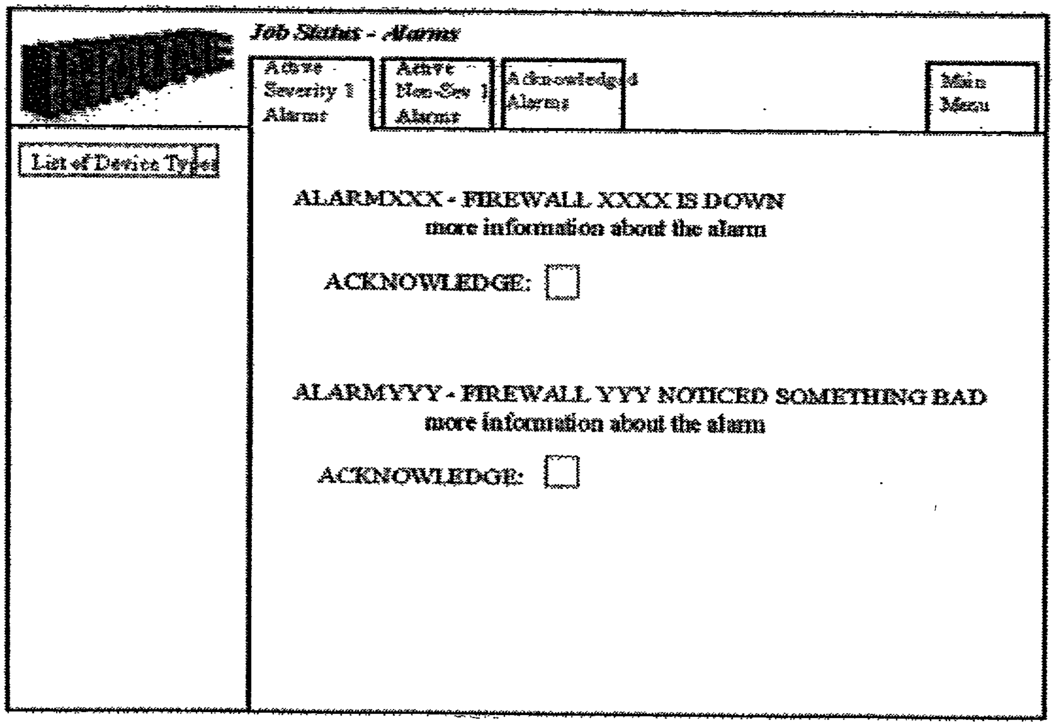
List of Logfile Types

SEARCH FOR A PARTICULAR EXPRESSION AND COUNT THE NUMBER OF LINES WHERE THE TEXT WAS FOUND.

STATUS	*REGULAR EXPRESSION*	*TEXT DESCRIPTION*
A/H	telnet.*connection for	Number of Telnet Connections
A/H	ftp.*connection for	Number of FTP Connections
A/H	ftp.*file	Number of FTP File Transfers
A	____________	____________
A	____________	____________

Save Changes

FIGURE 11



Job Status - Alarms

Active Severity 1 Alarms | Active Non-Sev 1 Alarms | Acknowledged Alarms | Main Menu

List of Device Types

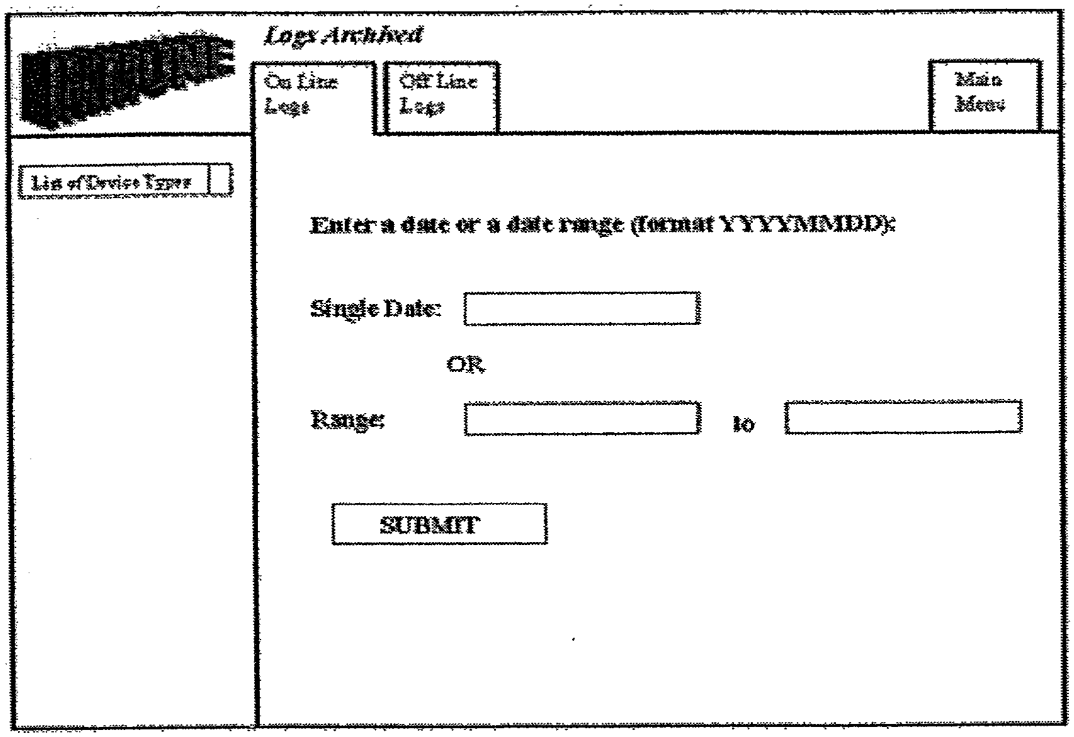
ALARMXXX - FIREWALL XXXX IS DOWN
more information about the alarm

ACKNOWLEDGE: □

ALARMYYY - FIREWALL YYY NOTICED SOMETHING BAD
more information about the alarm

ACKNOWLEDGE: □

FIGURE 12



Enter a date or a date range (format YYYYMMDD):

Single Date:

OR

Range: to

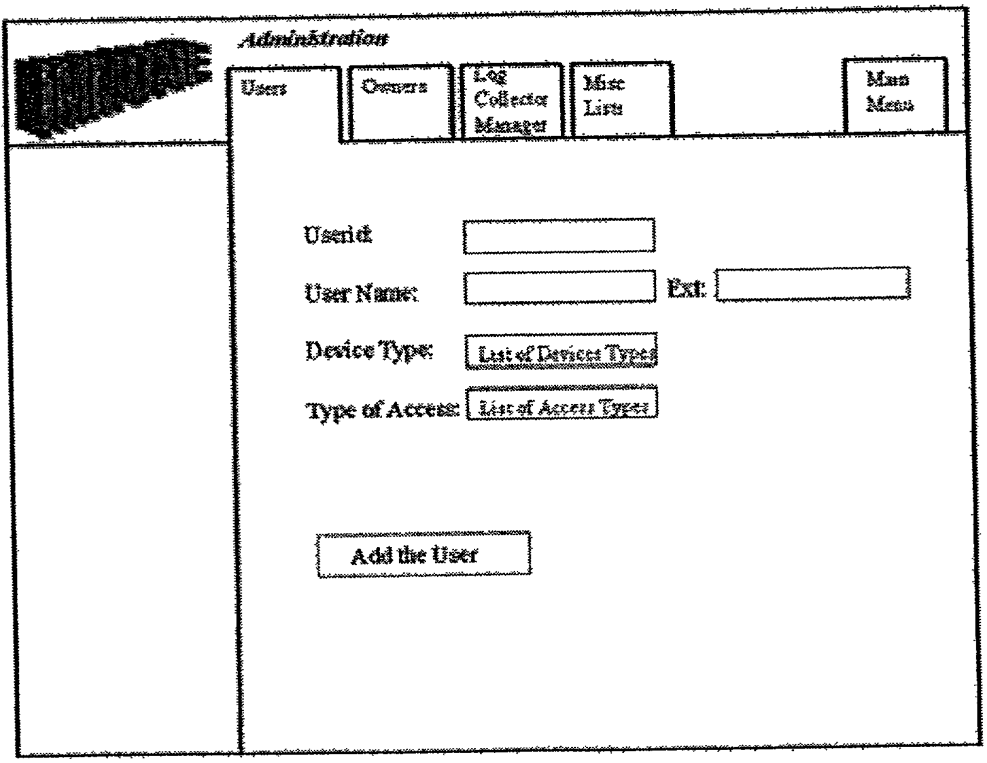
FIGURE 13.

To add a new user, the user must have a userid.

The entries in the device type list are taken from the device_types table.

The entries for the type of access are taken from the access_type table and are usually DBA, ANALYST.

More than one entry would be made if the user were able to see different device types. Ie. if they were able to see DBA for FIREWALLS, an entry would be made and if they were able to see ANALYST for SPAM, a separate entry would be made.



Userid:

User Name: Ext:

Device Type: List of Devices Types

Type of Access: List of Access Types

FIGURE 14.